

Le Darknet est régulièrement cité dans l'actualité, généralement en lien avec des affaires criminelles. À première vue, il s'agit d'un web "underground" infesté de trafiquants, de hackers et de pédophiles. Mais cette vision est réductrice. Le Darknet accueille également des défenseurs de la liberté d'expression, des blogueurs ou des lanceurs d'alertes qui fuient la censure et la répression.

Qu'est-ce que le Darknet?

Le Darknet est avant toute chose une masse de pages non indexées qu'il n'est pas possible de trouver avec les moteurs de recherche classiques ni avec un navigateur classique. Pour y accéder, il faut télécharger le logiciel Tor qui comporte un navigateur spécifique permettant d'accéder aux pages cachées du Darknet. Le système Tor fait transiter le trafic par plusieurs étapes, de manière à rendre la navigation impossible (ou très difficile) à tracer. En d'autres termes, en utilisant TOR, votre adresse IP ne peut plus être identifiée et personne ne peut connaître les pages que vous avez consultées.

Il est difficile d'estimer précisément la taille du Darknet. Certaines sources évoquent 600 Térabytes...

Le Darknet abrite une grande quantité de contenus illégaux: drogue, armes, pédopornographie, négationnisme... On peut également y trouver des "prestataires" d'actes illégaux ou criminels: hackers, tueurs à gages... Bref, le Darknet a un côté réellement "dark".

Pour le meilleur et pour le pire

Il serait abusif de résumer le Darknet à un repaire de criminels. Le Darknet abrite également beaucoup d'activistes, de journalistes ou de simples citoyens qui veulent défendre la liberté d'expression et ont besoin de se soustraire à la surveillance de masse ou à la censure de leur gouvernement.

Ainsi, on trouve un grand nombre de blogueurs chinois, de reportages et de photos sur la situation en Syrie ou en Ukraine, ou simplement de sites de promotion de la cryptographie.

Est-ce légal?

L'utilisation de TOR et l'accès au Darknet sont parfaitement légaux au Luxembourg, ce qui n'est pas le cas dans d'autres pays. Par contre, un certain nombre d'activités pratiquées sur ce réseau invisible sont illégales. En y accédant, il faut simplement se rappeler qu'acheter ou vendre certains produits ou services (drogue, armes, tueurs à gages...) est puni par la loi.

Est-ce sûr?

Tout dépend ce qu'on entend par "sûr". L'intérêt principal du Darknet est la confidentialité qu'il offre à ses utilisateurs. Par sa structure en oignon, plusieurs couches de chiffrement sont introduites entre l'utilisateur et les sites qu'il visite. Cela empêche normalement les espions et les agences de renseignement d'identifier des personnes utilisant les services du Darknet.

Cependant, la cyberpolice et les agences de renseignement sont également présentes sur le Darknet, pour essayer de remonter la trace des criminels. A priori, elles ne s'intéressent pas aux utilisateurs "normaux".

Concrètement, le browser Tor offre permet de naviguer en toute confidentialité. Ce browser introduit plusieurs couches de chiffrement entre l'utilisateur et les sites visités. Il existe d'autres moyens de se protéger sur internet, comme le VPN (virtual private network) qui crée un canal de communication chiffré.

Ensuite, il faut veiller à sécuriser son ordinateur et son browser, notamment en bloquant les scripts. En effet, de nombreux sites du Darknet utilisent le JavaScript pour de mauvaises raisons.

En pratique

Après avoir téléchargé le navigateur Tor, vous pouvez commencer à rechercher des adresses utiles avec l'extension .onion. C'est ici que les choses se compliquent, car il n'est pas évident de trouver un répertoire d'adresses valide et fiable. Pour vous faciliter la tâche, voici une sélection de liens testés que vous pourrez utiliser dans le navigateur Tor.

- Moteur de recherche : <http://hss3uro2hsxfogfq.onion>
- Hidden wiki: http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page
- Annuaire des liens : <http://torlinkbgs6aabns.onion>
- Facebook pour Tor: <https://facebookcorewwi.onion>
- Moteur de recherche Darknet: <http://grams7enufi7jmdl.onion>
- Vente des mobiles débloqués: <http://mobil7rab6nuf7vx.onion>
- Moteur de recherche DuckDuckGo: <http://3g2upl4pq6kufc4m.onion>

À côté du Darknet, il existe également différents types de "bibliothèques clandestines" qui visent souvent à publier des contenus littéraires ou scientifiques protégés par le droit d'auteur ou simplement non publiés dans les canaux traditionnels. Ces bibliothèques sont en général l'œuvre de personnes ou de groupes militants qui défendent le droit à l'information par opposition au droit d'auteur.

Quelques mises en garde:

Naviguer avec Tor sur des services où vous devez vous authentifier (réseaux sociaux, e-mail) est contre-indiqué. D'abord parce que cela supprime l'anonymat recherché. Mais aussi parce que vous risquez fort de déclencher des alertes de sécurité sur ces réseaux. En effet, ils auront l'impression que votre compte est corrompu parce qu'on essaye de s'y connecter à partir de points très éloignés les uns des autres...

Tor provoque un ralentissement de la navigation, justement à cause de la complexité du chemin emprunté par les données.

Tor ne constitue en aucun cas une protection contre les codes malicieux qui peuvent être présents sur certains sites ni contre le phishing par exemple.

Pour toute question au sujet de l'arnaque en ligne
ou sur l'utilisation d'Internet en général,
contactez la BEE SECURE Helpline:



August 16

powered by



La reproduction commerciale non modifiée et la distribution sont expressément autorisées.
<http://creativecommons.org/licenses/by-nc-nd/4.0/deed-fr/>



Éditeur : BEE SECURE · B.P. 707 · L-2017 Luxembourg
Tel.: (+352) 247-86427 · Fax.: (+352) 46 41 86
bee.secure@snj.lu · www.bee.secure.lu

